УДК 004.4

Ланде Д. В., Коцюба О. Ю., Рибак О. О.

Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського"

ВИЯВЛЕННЯ ДЖЕРЕЛ ДЕСТРУКТИВНОГО ІНФОРМАЦІЙНОГО ВПЛИВУ В МЕРЕЖІ ІНТЕРНЕТ

У цій роботі пропонується підхід до виявлення і візуалізації взаємозв'язку джерел деструктивного інформаційного впливу в мережі Інтернет, що базується на математичній лінгвістиці, кластерному аналізі і теорії графів. Практичне значення отриманих результатів полягає в створенні програмного забезпечення для вибору джерел інформації. Це надасть можливість подальшого застосування наведеної методології в задачах підтримки прийняття рішень.

It is proposed to develop an approach to identifying sources of destructive information impact on the Internet, based on mathematical linguistics, cluster analysis, and graph theory. The practical significance of the results obtained lies in the creation of software for the selection of information sources. This will allow the proposed methodology to be applied in decision support tasks.

На цей час ресурси мережі Інтернет стають домінуючим джерелом інформації для людей. В умовах жорстокої конкурентної боротьби, в процес інформування втручаються інформаційні джерела, що створюються з метою маніпулювання свідомістю людей. Враховується, що для максимального залучення уваги користувачів мережі маніпуляційні джерела найчастіше генерують повідомлення із заголовками, що містять спеціальну лексику, так званні меми, сенсаційні епітети тощо. Такі слова і словосполучення можуть виступати маркерами (індикаторами) маніпуляцій. Створення методології і інформаційних технологій виявлення джерел деструктивного інформаційного впливу в мережі Інтернет сьогодні актуально для задач змістовного аналізу мережевої інформації, дослідження суспільної думки, виявлення інформаційних атак і операцій, фільтрації впливу на людей.

Ця проблема сьогодні остаточно не розв'язана, їй займаються дослідники в усьому світі [1-4]. Побудова великих промислових систем виявлення маніпуляцій в електронних ЗМІ – це складна проблема, яка потребує великих ресурсних витрат.

Мета роботи – створення методології, теоретичних і технологічних засад виявлення джерел маніпулятивного інформаційного впливу в мережі Інтернет шляхом автоматизованого аналізу інформації із соціальних мереж.

Завдання полягає у розв'язанні часткових поставлених задач:

1. Аналіз існуючих підходів до визначення джерел інформаційного впливу через соціальні мережі.
2. Запропонувати та обґрунтувати алгоритми автоматизованого виявлення джерел маніпулятивного інформаційного впливу в мережі Інтернеті, визначення взаємозв'язків між джерелами, основних кластерів джерел інформаційного впливу.
3. Створити інструмент для виявлення і кластеризації джерел маніпулятивного інформаційного впливу через соціальні мережі.

Результати роботи можна використовувати для побудови системи вибору достовірних джерел інформації для задач підтримки прийняття рішень на основі моніторингу мережі Інтернет, в якості готового до застосування засобу виявлення і фільтрації маніпулятивних джерел інформації в умовах гібридних війн.

Методика виявлення джерел маніпулятивного інформаційного впливу в мережі Інтернеті, визначення взаємозв'язків між джерелами, основних кластерів джерел інформаційного впливу базується на лінгвістичному ймовірнісному підході, кластерному аналізі і теорії графів. Для реалізації методики застосовуються власні програмні компоненти, а також система аналізу і візуалізації графів Gephi (http://gephi.org) [5].

Основні етапи, що охоплює представлена методика – це етап навчання системи і етап сталого функціонування. Методика, таким чином реалізована у вигляді автоматизованої системи, що охоплює модулі навчання, модулі сталого функціонування і зовнішній пакет програм – систему Gephi. Обидва етапи системи пов'язані із ланцюжками взаємонезалежних кроків, зокрема, етап навчання системи полягає у створенні детального словника слів і словосполучень, що маркують маніпуляційні повідомлення, складається із:

1) Формування масиву вхідних повідомлень, що скануються із соціальних мереж [4] ;
2) Формування словника слів, що можуть маркувати повідомлення маніпулятивного характеру (термінів);
3) Фільтрація масиву вхідних повідомлень за допомогою цього словника;
4) Змістовний аналіз результатів фільтрації із застосуванням програмних компонентів виявлення найбільш значущих слів [6, 7] і коригування тимчасового словника.
5) Оформлення словника слів і словосполучень, що маркують маніпуляційні повідомлення.

Другий етап (сталого функціонування), містить такі кроки:

1) Фільтрація масиву вхідних повідомлень за допомогою детального словника слів і словосполучень, що маркують маніпуляційні повідомлення (враховуються тільки заголовки повідомлень);

2) Виведення назв і змісту джерела, що зустрічаються найчастіше всього,я для подальшого аналізу, як найбільш вірогідні маніпулятивні джерела інформації.
3) Визначення взаємозв'язку джерел маніпулятивної інформації. Для цього у відповідність кожному джерелу інформації ставиться вектор, елементи якого відповідають словнику слів і словосполучень, що маркують маніпуляційні повідомлення.
4) Матриця взаємозв'язку джерел завантажується у систему Gephi, де вона кластеризується і візуалізується (за класами модулярності) засобами цієї системи.

На останньому етапі формування і аналізу мережі взаємозв'язку джерел здійснюється її відображення за допомогою програмного пакету аналізу і візуалізації графів Gephi (https://gephi.org/). Для завантаження мережі джерел до баз даних цієї системи приведено відповідну матрицю суміжності до загальноприйнятого формату CSV.

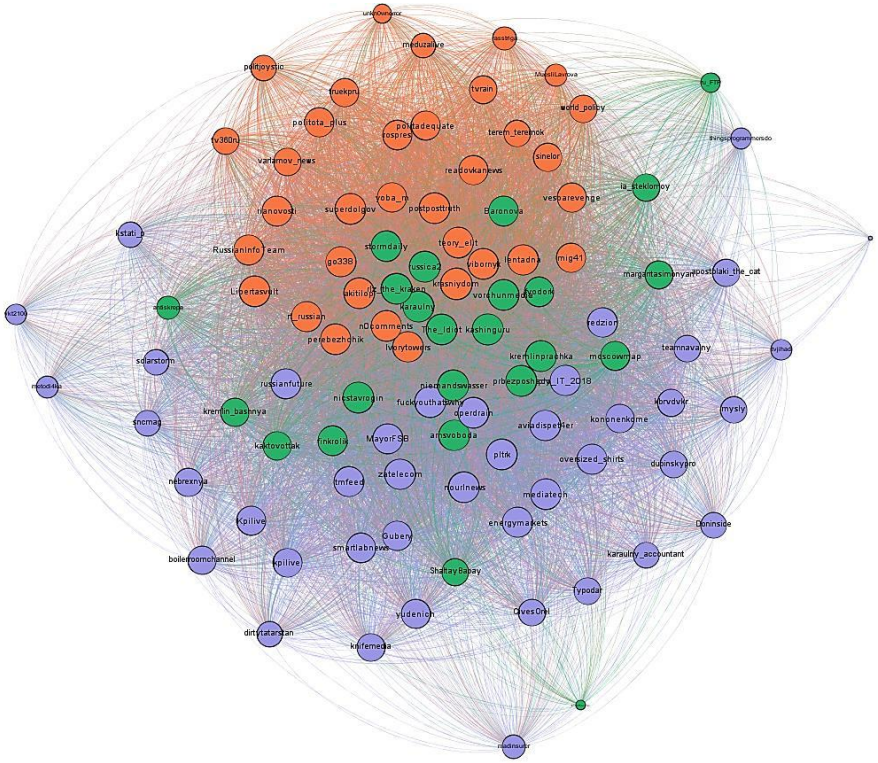

Рисунок 1 – Мережа джерел інформації у середовищі Gephi

Після завантаження файлу в середовище Gephi, засобами цієї системи здійснюється кластеризація вихідної мережі, обрахунок значень модулярності для кожного із кластерів, відображені статистичні дані мережі, де вузли відсортовані за класом модулярності, другий ключ сортування – ступінь вузла) і візуалізація мережі джерел інформації, що мають ознаки маніпуляційності (Рис. 1).

Отже, запропонована методологія автоматизованого виявлення джерел маніпулятивного інформаційного впливу в мережі Інтернеті та запропоновано новий метод визначення взаємозв'язків між джерелами та основних кластерів джерел інформаційного впливу. Практичне значення отриманих результатів полягає в створенні програмного забезпечення для автоматизованого вибору джерел інформації на основі моніторингу соціальних мереж, що надасть можливість подальшого застосування у задачах підтримки прийняття рішень. Крім того, розроблене програмно-алгоритмічне забезпечення можна використовувати на практиці в якості готового засобу виявлення і фільтрації маніпулятивних джерел інформації в умовах гібридних війн.

Перелік посилань

1. Conroy N.J., Rubin V.L., Chen Y. Automatic deception detection: Methods for finding fake news // asis&t, 2015. – Vol. 52, Iss. 1. – pp. 1-4. DOI: 10.1002/pra2.2015.145052010082.
2. Foreman J.W. Data Smart. Using Data Science to Transform Information into Insight. – Wiley, 2013. ISBN 111-8-66146-X, 978-1-11866-146-8.
3. Lazer D.M.J., Baum M.A., Benkler Y. etc. The science of fake news // Science, 2018. – Vol. 359, Iss. 6380. – pp. 1094-1096. DOI: 10.1126/science.aao2998
4. Ланде Д.В., Кальян Н.А., Матіїшин О.Т. Система контент-моніторингу соціальних мереж з питань кібербезпеки // "Інтелектуальний потенціал - 2019" - збірник наукових праць молодих науковців і студентів з нагоди 30-річчя кафедри кібербезпеки та комп'ютерних систем і мереж ХНУ/ - Хмельницький: ПВНЗ УЕП. - Ч.1: Комп'ютерні системи та кібербезпека, 2019. - С. 28-30.
5. Cherven K. Mastering Gephi Network Visualization. – Packt Publishing, 2015. ISBN 78-1-78398-734-4.
6. Lande D.V., Snarskii A.A., Yagunova E.V., Pronoza E.V. The Use of Horizontal Visibility Graphs to Identify the Words that Define the Informational Structure of a Text // 12th Mexican International Conference on Artificial Intelligence, 2013. - pp. 209-215.
7. Основи теорії і практики інтелектуального аналізу даних у сфері кібербезпеки: навчальний посібник / Д.В. Ланде, І.Ю. Субач, Ю.Є. Бояринова – Київ: ІСЗЗІ КПІ ім. Ігоря Сікрорського, 2018. - 300 с. ISBN 978-966-2577-12-9.